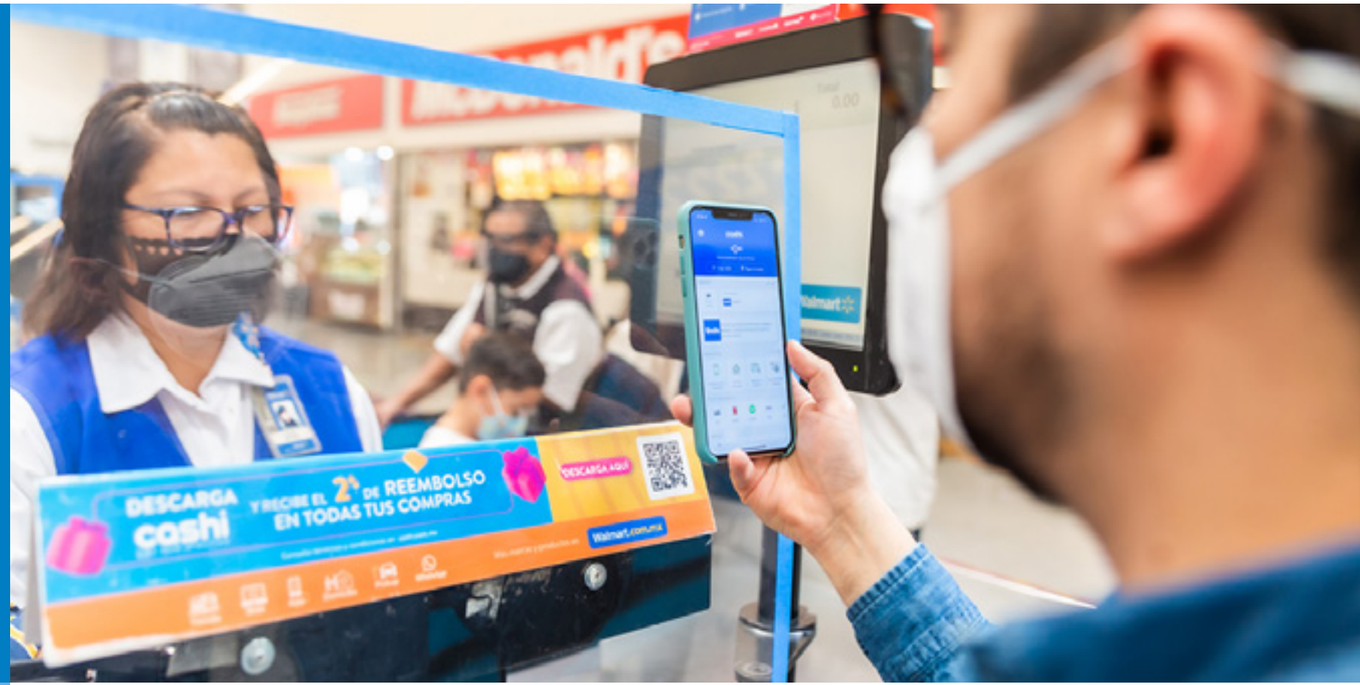
INFORMATION SECURITY

SASB FB-FR-230A.2, CG-MR-230A.1, CG-EC-230A.1



The information security program was created to provide our brand portfolio worldwide with comprehensive, profitable and risk-based security services

We guarantee protection for information and information systems against unauthorized access, use, alteration, modification, or destruction, thus providing confidentiality, integrity, and availability.

Our objective is to maintain company information secure through enhanced understanding of this subject and corresponding guidelines by our associates and business partners

We also ensure best practices are followed to identify risks, protect information, detect suspicious activities, in addition to being prepared to respond to future incidents.

Our company has policies, standards, procedures and information security guidelines, with the purpose of regulating and raising awareness among our associates and suppliers concerning the importance of the information and the technological resources used in the company. Our associates are offered training so they may better understand the importance of adopting behaviors in line with our information security guidelines.

Vulnerabilities present in company information assets are identified and managed with the following elements in mind: vulnerability-analysis scheduling; results documenting; and results classifying, with attention prioritization based on the severity of the risk.

Moreover, guidelines are provided for the design of vulnerability remediation plans; for penetration-testing protocols for critical assets; and for documentation of test results, requesting correction of any opportunities detected.

The time needed to create identities is reduced, thereby guaranteeing the uniqueness of over 170,000 associates. Furthermore, we guarantee faster access removal for those associates whose work contract has been terminated, in addition to having control over unauthorized access to tools and apps by suppliers.

Our Audit and Corporate Practices Committees are committed to the strategy of information security

Thus making the review process a fundamental part of their activities. A review is conducted every three months of all mitigation initiatives, trends, risks, and strategies. Furthermore, each market where we operate has its own information security leader who is also part of the committee that reviews and defines the cybersecurity strategy.

Our ecosystem is complex, as we handle millions of transactions per day. Each year we receive upwards of 1.5 billion global cyberattacks. Subsequently we have business continuity plans, enabling us to establish controls that supply the tools and resources needed to resume critical activities after any contingency jeopardizing operability of crucial processes by impacting the pillars of continuity: associates, facilities, systems, and third parties. Moreover, safety and surveillance incidents regarding the data extraction with unauthorized or coded devices are closely monitored.

In 2021, vulnerabilities were reduced by 57%, as compared to 2020. Annual certification from PCI Security Standards was obtained, with no findings noted. Our NIST CSF (National Institute of Standards and Technology Cyber Security Framework) maturity level was improved, going from 3.64 obtained in 2020, to 3.83 in 2021, where level 4 is the highest for this benchmark. We are working jointly with Infosec International on the consolidation of our response and prevention protocols to improve our reaction capabilities regarding any ransomeware attack.

Insofar as security, information requests on internal and external audits doubled. We were audited 22 times by the Internal Audit team and outside financial-sector agencies so we could provide proof of compliance regarding banking correspondence services, in addition to independent audits relative to NIST, Sarbanes & Oxley, and PCI (Payment Card Industry).